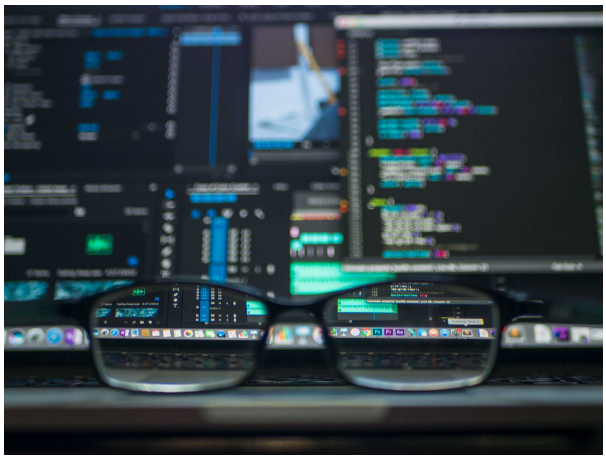
RANSOMWARE: The Single Biggest Threat to Any Individual or Business

by Kevin McDonald



I hope you will deeply consider what you are about to read. The sheer numbers and damage from Ransomware are no longer something you can avoid. If you don't already know someone with a ransomware horror story, it is very likely that you soon will. Ransomware is growing and most often strikes when you are least able to defend against it. The attackers come at night, on weekends and holidays when Information Technology staff and users are out relaxing. According to Cyber Security Ventures a new organization falls victim to ransomware every 14 seconds and that interval will reduce to 11 seconds by 2021. Close to 1 million ransomware infections were reported in 2019. Based on a poll of 500 businesses, Malwarebytes estimates that nearly 40% of all businesses were affected by a ransomware attack in 2019, a third of which lost revenue and 20% were forced to close their doors ...yes, as in out of business.

What are you talking about you ask? What is Ransomware anyway? It is the single biggest cyber threat to any individual or business today. Ransomware is a class of malware variants that encrypt data, making the data unusable without the passkey needed to unlock it. The attacker then offers to unlock the data after the victim pays a ransom within a specified amount of time. Paying may or may not ensure your data is accessible and paying will almost guarantee the attackers will return. Globally, about 40% of victims paid the ransom with an average demand of approximately $1,000 for individuals and $3, 000 per server in an enterprise attack. We have seen ransom demands associated with our rescues that were in the millions. We have also seen victims pay the ransom where their decryption process failed or took in excess of one year to decrypt. The tearful conversations are occurring weekly now. I listen to stories of how a victim is losing everything and in some cases there is nothing we can do for them. The attack severity and downtime have increased dramatically from our experience. In December for example, one company was forced to fire 300 employees due to a ransomware attack and many were financially strained due to lost business, client confidence and recovery costs.

A majority of those who got ransomware had a firewall and endpoint protection. The typical antivirus and malware protections simply do not work against a more

dedicated attacker with sophisticated tools. In many instances we find that several basic factors are at play. The attacker gained access to the victim's network either through exploiting an Internet facing or end-point vulnerability that was left unpatched, and a user clicking a link via email or social media. Some are being infected through drive by when simply visiting an infected webpage. Many of the cases we respond to were compromised through credential scraping malware that gets a username and password for a privileged account not protected by multi-factor authentication controls. That access is then used to patiently reconfigure systems, delete or encrypt the back-ups and then release the ransom demand. The average time an attacker was in a network we have seen is about three months but in some cases, the attackers were in the network much longer before they struck on a holiday.

If you don't already have a comprehensive ransomware defense and recovery strategy, you seriously need to start right now. Ransomware is very often not something that money or hard work can make go away. Hope and prayers will not bring your data back.

There are many reasons that recovery of the data becomes impossible. Some examples are:

1. You fail to pay or fail to pay on time and do not have a disaster recovery solution
2. The software installed or installation by the attacker is flawed and decryption does not work
3. An inexperienced IT team attempts to clean up the infection, damaging the ability to recover
4. The criminals, a government or law enforcement entity, takes down the decryption servers
5. The criminal decides not to provide the keys required for whatever reason

   In a growing number of cases, if you are able to recover without paying, the criminals have gathered sensitive information from your network for such an event. When you fail to pay, they threaten to release your sensitive information, whether it be private internal communications, consumer information or intellectual property. They attempt to extort money from you. If you do nothing else:

   1. Review accounts and limit what access they have to sensitive files
   2. Institute Multi-Factor Authentication ASAP
   3. Ensure all systems are patched for vulnerability

4. Segment your network to limit infection
5. Ensure you have a back-up and disaster plan that is current, disconnected from the primary network and using different user name and password with MFA are implemented
6. Train your users to NOT click links they are not 100% sure about source and security
7. Be sure you have complete and accurate documentation of your systems
8. Obtain adequate cyber liability and breach insurance
9. Put in place monitoring and response plans

The bottom line is you must assess your posture and ability to defend against Ransomware and network intrusion. You must be prepared to recover and you must act now before I or some other professional have another tearful conversation, but this time, about your losses.

Kevin B. McDonald, HCISPP is COO and CISO at Alvaka Networks. He has been with Alvaka Networks for nearly 18 years. Kevin is the appointed Chairman of the Orange County Sheriff/Coroner's Technology Advisory Council (T.A.C), a member of FBI Infragard, The High Tech Crimes Consortium and the US Secret Service's Electronic Crimes Task Force.

Kevin is a trusted technology and security expert and public policy advisor to some of America's most influential people and organizations. He advises corporate executives, federal and state legislators, law enforcement, high net worth individuals and other business leaders. He is a sought after consultant, writer, presenter and trainer. Kevin consults on the issues surrounding personal, physical and logical security, regulatory compliance and advanced technology.

Kevin has written for and/or been interviewed in dozens of national publications and television, radio and digital outlets such as CBS, Men's Health, CRN, CIO Insights, eWeek, Information Week, Information Security, Search Security, Network World, Computer World, and The Los Angeles Times.

alvaka.net